

HiveForce Labs

THREAT ADVISORY

 **VULNERABILITY REPORT**

Akira Ransomware Exploits Cisco Zero-Day Vulnerability

Date of Publication

September 11, 2023

Admiralty Code

A1

TA Number

TA2023363

Summary




Vulnerability Discovered: August 2023

Affected Products: Cisco Adaptive Security Appliance (ASA), Cisco Firepower Threat Defense (FTD)

Malware: Akira Ransomware

Impact: The zero-day vulnerability, identified as CVE-2023-20269, is a concerning security issue that impacts the remote access VPN feature of Cisco ASA (Adaptive Security Appliance) and FTD (Firepower Threat Defense). This remotely exploitable vulnerability, susceptible to brute force authentication, has been utilized by Akira Ransomware threat actors.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2023-20269	Cisco Brute Access Vulnerability	Cisco Adaptive Security Appliance (ASA) and Cisco Firepower Threat Defense (FTD)			

Vulnerability Details

#1

The CVE-2023-20269 zero-day vulnerability in Cisco Adaptive Security Appliance (ASA) and Cisco Firepower Threat Defense (FTD) is concerning because it is actively being exploited by ransomware operations to gain initial access to corporate networks. Akira Ransomware threat actor groups have specifically capitalized on this vulnerability and infiltrated several corporate network.

#2

The vulnerability affecting the VPN feature of Cisco allows unauthorized remote attackers to conduct brute force attacks against existing accounts, potentially leading to unauthorized access to the VPN service. These attacks compromised organizations that were using Cisco VPNs without multi-factor authentication (MFA) in place. The vulnerability had been previously identified during investigations into [Akira Ransomware](#) attacks.

#3

This vulnerability arises due to the inadequate separation of authentication, authorization, and accounting (AAA) mechanisms between the remote access VPN feature and the HTTPS management and site-to-site VPN features in Cisco ASA and Cisco FTD. Attackers can connect to the default connection profile/tunnel group through either a brute force attack or establish a clientless SSL VPN session with valid credentials.

#4

The vulnerability can be exploited through brute force attacks if an affected device has a user configured with a password stored in the local database, or if HTTPS management authentication is linked to a valid AAA server. Additionally, either SSL VPN or IKEv2 VPN must be enabled on at least one interface of the affected device for the vulnerability to be exploited.

#5

Successful exploitation enables attackers to acquire valid credentials through brute force attacks, subsequently granting them the ability to establish a VPN session. While a patch is currently unavailable, Cisco has provided workarounds to mitigate and manage the vulnerability.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-20269	Cisco Adaptive Security Appliance (ASA) 6.2.3 - 9.19.1.18 and Cisco Firepower Threat Defense (FTD) 6.2.3 - 9.19.1.18	cpe:2.3:h:cisco_systems:asa:6.2.3:*:*:*:*:*:* cpe:2.3:h:cisco_systems:firepower:6.2.3:*:*:*:*:*:*	CWE-288

Recommendations



Multi-Factor Authentication (MFA): Implement multi-factor authentication across all user accounts to strengthen access controls. This additional layer of security reduces the risk of unauthorized access, even if passwords are compromised.



Follow Workarounds: Follow the [workarounds](#) provided by Cisco to address the CVE-2023-20269 vulnerability. These workarounds closes the security gap that allows attackers to exploit vulnerability.



Dynamic Access Policies: Utilize Dynamic Access Policies (DAP) to prevent the establishment of VPN tunnels when the DefaultADMINGroup or DefaultL2LGroup connection profiles or tunnel groups are being used.



Restrict Users in the LOCAL User Database: Apply restrictions to the LOCAL user database by utilizing the 'group-lock' option to bind specific users to a single profile. Simultaneously, ensure that VPN setups are prohibited by configuring 'vpn-simultaneous-logins' to zero.



Potential MITRE ATT&CK TTPs

<u>TA0001</u> Initial Access	<u>TA0004</u> Privilege Escalation	<u>TA0006</u> Credential Access	<u>TA0002</u> Execution
<u>TA0011</u> Command and Control	<u>TA0009</u> Collection	<u>TA0003</u> Persistence	<u>T1005</u> Data from Local System
<u>T1133</u> External Remote Services	<u>T1078</u> Valid Accounts	<u>T1078.003</u> Local Accounts	<u>T1068</u> Exploitation for Privilege Escalation
<u>T1110</u> Brute Force	<u>T1059</u> Command and Scripting Interpreter	<u>T1059.008</u> Network Device CLI	<u>T1572</u> Protocol Tunneling

Indicators of Compromise (IOCs)

TYPE	VALUE
IPs	161.35.92[.]242, 173.208.205[.]10, 185.157.162[.]21, 185.193.64[.]226, 149.93.239[.]176, 158.255.215[.]236, 95.181.150[.]173, 94.232.44[.]118, 194.28.112[.]157, 5.61.43[.]231, 5.183.253[.]129 45.80.107[.]220, 193.233.230[.]161, 149.57.12[.]131, 149.57.15[.]181, 193.233.228[.]183, 45.66.209[.]122, 95.181.148[.]101, 193.233.228[.]86, 176.124.201[.]200, 162.35.92[.]242, 144.217.86[.]109, 31.184.236[.]63, 31.184.236[.]71,

IPv4

31.184.236[.]79,
194.28.112[.]149,
62.233.50[.]19,
194.28.112[.]156,
45.227.255[.]51,
185.92.72[.]135,
80.66.66[.]175,
62.233.50[.]11,
62.233.50[.]13,
194.28.115[.]124,
62.233.50[.]81,
152.89.196[.]185,
91.240.118[.]9,
185.81.68[.]45,
152.89.196[.]186,
185.81.68[.]46,
185.81.68[.]74,
62.233.50[.]25,
62.233.50[.]17,
62.233.50[.]23,
62.233.50[.]101,
62.233.50[.]102,
62.233.50[.]95,
62.233.50[.]103,
92.255.57[.]202,
91.240.118[.]5,
91.240.118[.]8,
91.240.118[.]7,
91.240.118[.]4,
161.35.92[.]242,
45.227.252[.]237,
147.78.47[.]245,
46.161.27[.]123,
94.232.43[.]143,
94.232.43[.]250,
80.66.76[.]18,
94.232.42[.]109,
179.60.147[.]152,
185.81.68[.]197,
185.81.68[.]75

Workarounds

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asafth-ravpn-auth-8LyfCkeC#workarounds>

References

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asafth-ravpn-auth-8LyfCkeC#vp>

<https://www.hivepro.com/new-wave-of-akira-ransomware-expands-arsenal-with-cisco-vpn-flaws/>

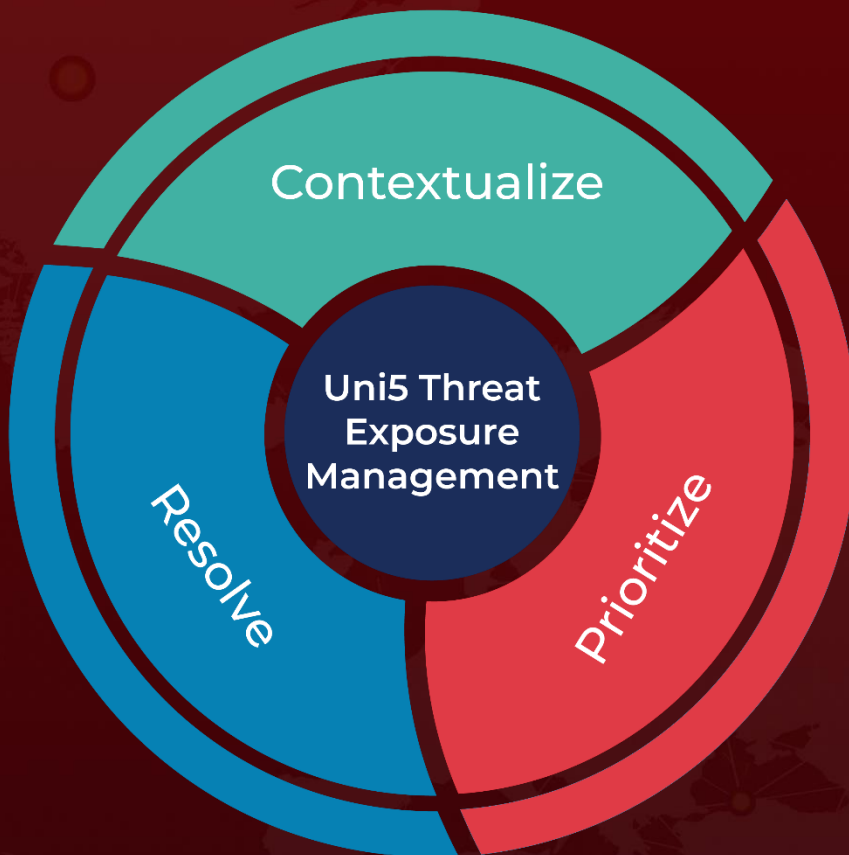
<https://blogs.cisco.com/security/akira-ransomware-targeting-vpns-without-multi-factor-authentication>

<https://www.rapid7.com/blog/post/2023/08/29/under-siege-rapid7-observed-exploitation-of-cisco-asa-ssl-vpns/>

What Next?

At Hive Pro, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with HivePro Uni5: Threat Exposure Management Platform.



REPORT GENERATED ON

September 11, 2023 • 8:10 AM

© 2023 All Rights are Reserved by HivePro®



More at www.hivepro.com